US006167514A

United States Patent [19]

Matsui et al.

[11] Patent Number: 6,167,514

[45] Date of Patent: Dec. 26, 2000

[54] **METHOD, APPARATUS, SYSTEM AND INFORMATION STORAGE MEDIUM FOR WIRELESS COMMUNICATION**

[75] Inventors: **Tetsuya Matsui; Michio Kobayashi; Masaki Hoshina**, all of Suwa, Japan

[73] Assignee: **Seiko Epson Corporation**, Tokyo, Japan

[21] Appl. No.: **09/029,719**

[22] PCT Filed: **Jul. 3, 1997**

[86] PCT No.: **PCT/JP97/02303**

§ 371 Date: **Mar. 26, 1998**

§ 102(e) Date: **Mar. 26, 1998**

[87] PCT Pub. No.: **WO98/01975**

PCT Pub. Date: **Jan. 15, 1998**

[30] **Foreign Application Priority Data**

Jul. 5, 1996 [JP] Japan 8-195708

[51] **Int. Cl.**[7] **G06N 17/00**

[52] **U.S. Cl.** **713/150**; 713/168; 713/169; 713/170; 380/255; 380/264; 380/270

[58] **Field of Search** 380/255, 258, 380/264, 270, 277, 278; 713/168, 169, 170, 171, 150

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,016,276 5/1991 Matumoto et al. .

FOREIGN PATENT DOCUMENTS

A1 0 695 059	1/1996	European Pat. Off. .
63-36634	2/1988	Japan .
7-104956	4/1995	Japan .
7-210644	8/1995	Japan .
8-36534	2/1996	Japan .
8-65303	3/1996	Japan .
8-65306	3/1996	Japan .
WO 95/19015	7/1995	WIPO .
WO 96/04734	2/1996	WIPO .

OTHER PUBLICATIONS

Menezes et al., "Handbook of Applied Cryptography", 1965, pp. 491, 497, 498.

T. Matsumoto et al., "Key Predistribution System*, Key Sharing without Communication: The Key Predistribution Systems," Transactions of Inst. of Electronics, Inform. and Comm. Engineers A, vol. J71–A, No. 11, 1988, pp. 2046–2053.

S. Miyafuchi, "Does KPS Protect Privacy?", Electronics, Sep. 1995, pp. 51–53.

T. Matsumoto et al., "A Prototype KPS and Its Application–IC Card Based Key Sharing and Cryptographic Communication," Transactions of Institute of Electronics, Inform. and Comm. Engineers, vol. E73, No. 7, 1990, pp. 1111–1119.

T. Matsumoto et al., "Sharing of Encryption Key, Key Sharing System KPS for Large–Scale Networks and Its Realization," Technical Research Report of IEICE, vol. 89, No. 482, (ISEC89–52), 1990, pp. 33–47.

M. Yamai, "Ethernet and TCP/IP," Open Design, vol. 1, No. 3, 1994, pp. 1–32.

Primary Examiner—Thomas R. Peeso

Attorney, Agent, or Firm—Oliff & Berridge, PLC

[57] **ABSTRACT**

Wireless communication method and apparatus which can perform the wireless transmission/reception of encrypted data without previous provision of a cryptographic key and without any system for registering a cryptographic key. Under control of a communication control section **504** in PC **1**, the PC **1** transmits its own identification information to a printer **2** and receives identification information of the printer **2**. The PC **1** has an encrypting/decrypting section **502** which generates a cryptographic key by using the identification information of the printer **2** and its own secret algorithm read out of an identification information storage section **510**. According to a cryptographic program using such a cryptographic key, data is encrypted and transmitted toward the printer **2**.

23 Claims, 14 Drawing Sheets